IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION of
Inventor(s): LIM

Appln. No.:	09	866,874
Series Code	↑	↑ Serial No.

Group Art Unit: Not Assigned

Filed: May 30, 2001

Examiner: Not Assigned

Title: ENCRYPTION DEVICE USING DATA ENCRYPTION STANDARD ALGORITHM

Atty. Dkt. P 281290 | P00HA006/US

M# | Client Ref

Date: August 2, 2001

SUBMISSION OF PRIORITY DOCUMENT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 55

Hon. Asst Commissioner of Patents
Washington, D.C. 20231

Sir:

Please accept the enclosed certified copy(ies) of the respective foreign application(s) listed below for which benefit under 35 U.S.C. 119/365 has been previously claimed in the subject application and if not is hereby claimed.

Application No.	Country of Origin	Filed
2000-31574	KOREA	June 9, 2000
2000-29631	KOREA	May 31, 2000

Respectfully submitted,

Pillsbury Winthrop LLP
Intellectual Property Group

1600 Tysons Boulevard
McLean, VA 22102
Tel: (703) 905-2000
Atty/Sec: gjp/JRH

By Atty: Glenn J. Perry **Reg. No.** 28458

Sig:

Fax: (703) 905-2500
Tel: (703) 905-2161

PILLSBURY WINTHROP LLP

1600 TYSONS BOULEVARD MCLEAN, VA 22102 703.905.2000 F: 703.905.2500

August 2, 2001

Glenn J. Perry
703.905.2161
gjperry@pillsburywinthrop.com

Mr. Seok-Hee Wonn
Shinsung International Patent & Law Firm
Kangnam P.O. Box 1374
Seoul 135-613
KOREA

Re: U.S. Application of LIM
Appln. No.: 09/866,874
Your Ref.: P00HA006/US
Our Ref.: GJP/82123/281290

Dear Mr. Wonn:

Thank you for your order letter of May 30, 2001 enclosing the application and the priority documents. In accordance with your instructions, we prepared and filed an application for U.S. patent from the e-mail specification and drawings on June 6, 2001 and enclose two copies of this filing for your records. We apologize for the delay in reporting this filing, but our office move to Northern Virginia in mid-June has caused unusual delays in our normal workflow. We appreciate your patience and understanding.

Because we filed the application from the e-mail specification and drawings, we did not have the Priority Document at the time the application was filed. Thus, we filed the Priority Documents on August 1, 2001, and enclose two copies of that filing for your records as well. Our debit note for both filings will follow shortly with the confirmation copy of this letter.

We look forward to receiving the executed Declaration and Assignment for this application. We will let you know when we receive the Notice of Missing Parts.

Very truly yours,

Glenn J. Perry

GJP:jrh

Enclosures

<Priority Document Translation>

THE KOREAN INDUSTRIAL

PROPERTY OFFICE

This is to certify that annexed hereto is a true copy from the records of the Korean Industrial Property Office of the following application as filed.

Application Number : 2000-31574 (Patent)

Date of Application : June 9, 2000

Applicant(s) : HYUNDAI ELECTRONICS INDUSTRIES CO., LTD.

October 30, 2000

COMMISSIONER

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 29631 호
Application Number

출 원 년 월 일 : 2000년 05월 31일
Date of Application

출 원 인 : 현대전자산업주식회사
Applicant(s)

CERTIFIED COPY OF PRIORITY DOCUMENT

2000 년 10 월 30 일

특 허 청
COMMISSIONER

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【제출일자】 2000.06.09
【발명의 명칭】 데이터 암호화 표준 알고리즘을 이용한 암호화 장치
【발명의 영문명칭】 Encryption device using data encryption standard algorithm

【출원인】
【명칭】 현대전자산업주식회사
【출원인코드】 1-1998-004569-8
【대리인】
【성명】 박해천
【대리인코드】 9-1998-000223-4
【포괄위임등록번호】 1999-008448-1
【대리인】
【성명】 원석희
【대리인코드】 9-1998-000444-1
【포괄위임등록번호】 1999-008444-1
【발명자】
【성명의 국문표기】 임영원
【성명의 영문표기】 LIM,Young Won
【주민등록번호】 621128-1067119
【우편번호】 467-850
【주소】 경기도 이천시 대월면 현대전자사원아파트 106-1302
【국적】 KR
【심사청구】 청구
【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
박해천 (인) 대리인
원석희 (인)

【수수료】
【기본출원료】 20 면 29,000 원
【가산출원료】 6 면 6,000 원

【우선권주장료】	0	건	0 원
【심사청구료】	3	항	205,000 원
【합계】	240,000 원		
【첨부서류】	1. 요약서·명세서(도면)_1통		

【요약서】

【요약】

본 발명은 두 개의 S-Box 치환부를 2-포트의 입력을 가진 장치로 구현한 데이터 암호화 표준 알고리즘을 이용한 암호화 장치에 관한 것으로, 면적을 최소화하고 성능을 증대시킬 수 있는 암호화 장치를 제공하는데 그 목적이 있다. 이를 위하여 본 발명은 데이터 암호화 표준 알고리즘을 사용하여 암호화를 수행하는 암호화 장치에 있어서, 제1제어기의 제어를 받아 입력되는 48 비트의 제1입력과 제2입력 중에서 하나를 선택하는 제1멀티플렉서; 상기 제1멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 제1S-Box; 제1제어기의 제어를 받아 상기 4비트의 데이터를 두개로 분배하는 제1디멀티플렉서; 제1클럭과 제2클럭을 입력받아 상기 제1멀티플렉서와 제1디멀티플렉서를 제어하는 제1제어기; 제2제어기의 제어를 받아 입력되는 48 비트의 제3입력과 제4입력 중에서 하나를 선택하는 제2멀티플렉서; 상기 제2멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 제2S-Box; 제2제어기의 제어를 받아 상기 4비트의 데이터를 두개로 분배하는 제2디멀티플렉서; 제1클럭과 제2클럭를 입력받아 상기 제2멀티플렉서와 제2디멀티플렉서를 제어하는 제2제어기를 포함하여 이루어진다.

【대표도】

도 8

【색인어】

제1멀티플렉서, 제1S-Box, 제1디멀티플렉서, 제1제어기, 제2멀티플렉서, 제2S-Box, 제2디멀티플렉서, 제2제어기

【명세서】

【발명의 명칭】

데이터 암호화 표준 알고리즘을 이용한 암호화 장치{Encryption device using data encryption standard algorithm}

【도면의 간단한 설명】

도1는 일반적인 DES 아키텍처의 사이퍼 함수와 S-Box 치환부의 상세한 구성도,

도2은 종래기술의 8 단의 파이프라인 구조의 DES 아키텍처를 나타낸 블럭도,

도3는 종래 기술의 8단 파이프라인 구조의 DES 아키텍처의 동작 순서를 나타내는 타이밍도,

도4은 종래 기술의 8단의 파이프라인 구조의 DES 아키텍처의 파이프라인 동작 순서를 나타내는 타이밍도,

도5는 종래 기술에서 8단의 파이프라인 구조의 DES 아키텍처로써, 파이프라인을 사용한 경우와 사용하지 않은 경우에 사이퍼 함수가 연산되는 순서도,

도6은 종래기술의 8단의 파이프라인 구조의 DES 아키텍처에서 단일 포트 S-Box 치환부의 구현 방식을 나타낸 상세한 블럭도,

도7은 종래기술의 8단의 파이프라인 DES 아키텍처에서 4-포트 S-Box 치환부의 구현을 나타낸 블럭도,

도8은 본 발명의 두 개의 2-포트 S-Box 치환부를 나타내는 블럭도,

도9은 종래 방식의 단일 포트 S-Box 치환부와 4포트 S-Box 치환부 그리고 본 발명의 2-포트 S-Box 치환부의 동작을 나타내는 타이밍도.

* 도면의 주요 부분에 대한 부호의 설명 *

810 : 제1멀티플렉서	820 : 제1S-Box
830 : 제1디멀티플렉서	840 : 제1제어기
850 : 제2멀티플렉서	860 : 제2S-Box
870 : 제2디멀티플렉서	880 : 제2제어기

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<15> 본 발명은 암호화 장치에 관한 것으로, 특히 데이터 암호화 표준 알고리즘을 이용한 암호화 장치에 관한 것이다.

<16> 일반적으로 데이터 암호화 표준(DES : Data Encryption Standard, 이하 DES라 칭함) 알고리즘은 가장 널리 쓰이고 있는 암호화 방식으로 네트워킹 사용이 증가함에 따라 그 중요성을 더해 가고 있다. 특히, 보안 인터넷 응용이나 원격 접근 서버나 케이블 모뎀과 위성용 모뎀 등의 분야에서 많이 이용되고 있다.

<17> DES는 기본적으로 64비트 블럭의 입력 및 출력을 가지는 64비트 블럭 암호이며, 64비트의 키 블럭 중 56비트가 암호화 및 복호화에 사용되고, 나머지 8비트는

패리티 검사용으로 사용된다. 또한. 64비트의 평문(Plain Text) 블럭과 56비트의 키(Key)를 입력으로 해서 64비트의 암호문(Ciper Text) 블럭을 출력하는 암호화 장치이다.

<18> DES를 실현시키는 중요한 기법은 치환(P-Box), 대치(S-Box) 그리고 보조키(Subkey)를 발생시키는 키 스케쥴 등이 있다.

<19> 데이터 암호화부의 내부는 16라운드의 반복연산을 수행하는 형태로 되어 있고 입력부의 초기 치환(IP)와 출력부의 역초기 치환(IP^{-1})으로 구성되어 있다.

<20> 도1는 일반적인 DES 아키텍쳐의 사이퍼 함수와 S-Box 치환부의 상세한 구성도이다.

<21> 상기 도1을 참조하면, 사이퍼 함수 f는 32비트의 텍스트 블럭을 저장하고 있는 오른쪽레지스터로부터 32비트의 데이터(R(i-1))를 입력받아 48비트의 데이터로 확장 치환하는 확장치환부(110)와, 상기 확장치환부의 48비트의 데이터를 입력받고 키 스케쥴(Key Schedule)로부터의 보조키(K_i)를 입력받아 배타적 논리합 연산을 수행하는 익스쿠르시브-오아부(120)와, 상기 익스쿠르시브-오아부(120)로부터의 48비트의 데이터를 32비트의 데이터로 대치 치환하는 S-Box 치환부(130)와, 상기 S-Box 치환부(130)의 32비트의 데이터를 복사 치환하는 P-Box 치환부(140)와, 상기 P-Box 치환부의 32비트의 데이터와 왼쪽레지스터에 저장되어 있는 32비트의 데이터(L(i-1))를 입력받아 배타적 논리합하는 익스쿠르시브-오아부(150)를 구비한다.

<22> 키 스케쥴(Key Schedule)은 56비트의 키(Key)를 입력받아서 28비트의 두 블럭으로 나누어서 각각 왼쪽으로 한자리 또는 두자리씩 쉬프트하는 쉬프트부(160, 170)와 상기 쉬프트부의 두 블럭을 입력받아 하나의 보조키로 압축하여 치환하는 압축치환부(180)를

구비한다.

<23> 구체적으로, 상기 S-Box 치환부는 48비트의 입력을 받아서 32비트의 출력을 생성하는 8 개의 S-Box로 구성되어 있다. 즉, 48비트의 데이터는 8 개의 6비트 데이터로 분할되어 8 개의 S-Box에 입력된다. 이 8 개의 S-Box들은 8 개의 출력을 내보냄으로써 48 비트를 32비트로 줄인다. S-Box 치환부(130)는 테이블 룩-업(Look-up) 방식으로 대치됨으로써 프로그램가능 논리 어레이(PLA)나 롬(ROM)과 같은 기억장치를 필요로 한다. 6비트의 입력에 대하여 4비트를 출력하기 때문에 각 S-Box는 64 ×4 의 기억 용량이 필요하며 전체적으로 8개의 S-Box로 구성되어 있으므로 8 ×64 ×4의 기억장치가 필요하다.

<24> 도2은 종래기술의 8 단의 파이프라인 구조의 DES 아키텍쳐를 나타낸 블럭도이다.

<25> 상기 도2을 참조하면, 종래기술의 DES 알고리즘은 초기 치환부를 거친 64비트의 평문(Plain Text) 블럭을 32비트의 두 블럭으로 나뉘어 a_0와 b_0를 제1클럭과 제2클럭을 사용하여 제1왼쪽레지스터(A0)(260)와 제1오른쪽레지스터(B0)(200)에 저장한 후, 키 스케쥴(Key Schedule)로부터 생성된 보조키($K_{(i)}$)를 입력받아 상기 제1오른쪽레지스터로부터의 32비트의 데이터를 사이퍼 함수 f_B(210)에 의해서 암호화 변형하며, 상기 사이퍼 함수 f_B에 의해 변형된 32비트의 데이터를 상기 제1왼쪽레지스터(A0)(260)의 32비트와 익스쿠르시브-오아부(220)에서 배타적 논리합 연산을 수행한다. 또한, 상기 익스쿠루시브-오아부의 32비트 데이터를 제1클럭(CLK1)을 사용하여 제2왼쪽레지스터(A1)(230)에 저장하고, 보조키($K_{(i+1)}$)를 입력받아 상기 제2왼쪽레지스터에저장되어 있는 32비트의 데이터를 사이퍼 함수 f_C(240)를 통하여 변형하며, 변형된 32비트의 데이터를 상기 제1오른쪽레지스터(B0)(200)의 32비트와 익스쿠르시브-오아부(250)에서 배타적 논리합 연산을 수행한다. 이와 같은 2 개의 라운드가 반복되어 8개의 라운드가 구성되고 마지막 라운드의

제1왼쪽레지스터(A0)(260)의 32비트가 b_{15}가 되며 마지막 라운드의 익스쿠르시브-오아부(270)에서 출력된 32비트가 b_{16}이 된다.

<26> 왼쪽에 있는 레지스터는 A1, A2, A3, A0으로, 오른쪽에 있는 레지스터는 B0, B1, B2, B3으로 표시하였다. 도1과 같이 레지스터 A0, A1, A2, A3는 제1클럭(CLK1)을 사용하여 데이터를 저장하고 레지스터 B0, B1, B2, B3는 제2클럭(CLK2)을 사용하여 데이터를 저장한다. 제2클럭(CLK2)는 제1클럭(CLK1)을 반전시킨 것으로 제1클럭(CLK1)의 반주기만큼 지연된 것으로 볼 수 있다.

<27> 도3는 종래 기술의 8단 파이프라인 구조의 DES 아키텍처의 동작 순서를 나타내는 타이밍도이다.

<28> 상기 도3을 참조하면, 32비트의 블럭 a_0와 b_0는 초기 치환을 거친 64비트의 평문 블럭이 32비트의 두블럭으로 나뉘어진 것이고, 32비트의 블럭 a_0는 왼쪽변수(L_0)가 되며 32비트의 블럭 b_0는 오른쪽변수(R_0)가 된다. 그리고 DES 코아가 계산하는 값을 b_1, b_2 ....b_{16} (b_i=R_i)라고 하고 키 스케쥴러(Ker Scheduler)가 주기적으로 보조키 K_i를 사이퍼 함수 f에 입력해주도록 제어기를 만들면 32비트 블럭 b_i의 값을 계산하는 과정은 다음과 같다.

<29> 먼저 t_0와 t_1에서 a_0와 b_0 값이 레지스터 A0와 B0에 제1클럭(CLK1)과 제2클럭(CLK2)에 의해서 각각 저장된다. t_1에서부터 b_1값(b_1 = a_0

⊕ $f(b_0,K_1)$)을 계산하기 시작해서 t_2에서 계산된 값을 레지스터 A1에 저장한다. 이 때 레지스터 A0에 입력된 값 a_0는 t_2까지만 유지가 되면 t_1-t_2구간에서 b_1값을 계산하는데 사용할 수 있다. 이 것은 반전된 제1클럭(CLK1)과 제2클럭(CLK2)에 의해서 레지스터 A1과 B0가 새로운 값을 저장하기 때문에 해결할 수 있다. 즉 레지스터 A1이 새로운 데이터를 저장할 수 있는 시간은 t_0, t_2, t_4 ....이고 레지스터 B0에 새로운 데이터가 입력되는 시간은 t_1, t_3, t_5 ....이다. 마찬가지로 t_1에서 레지스터 B0에 저장된 값 b_0와 t_2에서 레지스터 A1에 저장된 값 b_1이 t_2-t_3구간에서 유지되기 때문에 t_3에서 레지스터 B1에 상기 제2클럭(CLK2)를 사용하여 계산된 b_2 값($b_2 = b_0 \oplus f(b_1, K_1)$)을 저장할 수 있다. 이와 같은 방식으로 상기 제1클럭(CLK1)이 상승할 때 t_0, t_8, t_{16} 에서 a_0, b_7, b_{15}값이 레지스터 A0에, t_2, t_{10}에서 b_1, b_9값이 레지스터 A1에, t_4, t_{12}에서 b_3, b_{11}값이 레지스터 A2에, t_6, t_{14}에서 b_5, b_{13}값이 레지스터 A3에 각각 저장된다. 또한 상기 제2클럭(CLK2)가 상승할 때 t_1, t_9, t_{17}에서 b_0, b_8, b_{16}값이 레지스터 B0에, t_3, t_{11}에서 b_2, b_{10}값이 레지스터 B1에, t_5, t_{13}에서 b_4, b_{12}값이 레지스터 B2에, t_7, t_{15}에서 b_6, b_{14}값이 레지스터 B3에 각각 저장된다. 일반적인 DES 코아는 16 라운드를 수행하기 때문에 16 클럭 사이클이 걸리나 상기의 8단 파이프라인 구조의 DES 아키텍처의 종래기술에서는 t_0에서 a_0가 저장되기 시작해서 b_{16}이 계산되어 출력하기까지 8.5 클럭 사이클이 걸린다.

<30> 일반적으로 주어진 키(Key)에 대하여 암호화 또는 해독화 해야 될 다수의 64비트 평문 블럭이 연속적으로 입력되는 경우가 많다.

<31> 도4은 종래 기술의 8단의 파이프라인 구조의 DES 아키텍처의 파이프라인 동작 순서를 나타내는 타이밍도이다.

<32> 상기 도4을 참조하면, 네개의 평문 블럭들을 8.5 클럭 사이클 동안에 동시에 처리할 수 있음을 보여준다. 도3에서 비어 있는 부분에 새로운 평문 블럭 c_0와 d_0를 t_2와 t_3에서, e_0와 f_0를 t_4와 t_5에서, g_0와 h_0를 t_6과 t_7에서 각각 레지스터 A0와 B0에 입력함으로써 b_i값들을 계산하는 동안 d_i, f_i, h_i값들을 계산할 수 있음을 보여준다. 이 때 t_0-t_1,t_1-t_2, t_2-t_3,... 구간마다 새로운 b_i, d_i, f_i, h_i값을 얻기 위해 사이퍼 함수 f가 네개씩 동시에 수행된다. 따라서 주어진 클럭 사이클 동안에 처리할 수 있는 평문 블럭의 수는 네 배로 증가 시킬 수 있으나, S-Box 치환부를 세 개씩 추가로 구현하여야 한다는 단점이 있다.

<33> 도5는 종래 기술에서 8단의 파이프라인 구조의 DES 아키텍쳐로써, 파이프라인을 사용한 경우와 사용하지 않은 경우에 사이퍼 함수가 연산되는 순서도이다.

<34> 상기 도5를 참조하면, 한개의 64비트 평문 블럭을 암호화하는 경우 즉, 파이프라인을 사용하지 않을 경우는 도2의 8개의 사이퍼 함수 f_A, f_B, f_C, f_D, f_E, f_F, f_G, f_H 는 두개의 위상을 갖는 클럭에 의해서 시분할이 되어 계산되기 때문에 1 개의 S-Box 치환부만으로도 구현가능하다. 그러나 파이프라인을 사용하여 네 개의 64비트의 평문 블럭을 동시에 암호화할 경우에 (f_A, f_C, f_E, f_G)와 (f_B, f_D, f_F, f_H)는 서로 시분할되지만 (f_A, f_C, f_E, f_G)와 (f_B, f_D, f_F, f_H)는 시분할이 되지 않고 동시에 계산되기 때문에 네 개의 S-Box가 필요하다.

<35> 도6은 종래기술의 8단의 파이프라인 구조의 DES 아키텍쳐에서 단일 포트 S-Box 치환부의 구현 방식을 나타낸 상세한 블럭도이다.

<36> 상기 도6을 참조하면, 종래기술의 S-Box 치환부는 네 개를 사용하여 파이프라인 동작을 수행하도록 되어 있고, 하나의 S-Box 치환부는 48비트의 입력 데이터를 받아들여

32비트의 출력 데이터를 내보내는 8 개의 S-Box로 구성되어 있다. 각각의 S-Box는 64 × 4 의 롬(ROM)이나 프로그램가능 논리 어레이(PLA)로 구성되어 있고 6비트의 어드레스를 입력받아 4비트의 데이터를 출력하는 제1경로(path1)를 구비하고 있다. 네개의 S-Box 치환부에는 서로 다른 제1경로(path1)와 제2경로(path2)와 제3경로(path3)와 제4경로(path4)가 물리적으로 존재한다.

<37> 도7은 종래기술의 8단의 파이프라인 DES 아키텍쳐에서 4-포트 S-Box 치환부의 구현을 나타낸 블럭도이다.

<38> 상기 도7을 참조하면, 종래기술의 S-Box 치환부는 제어기의 제어를 받아 입력되는 네 개의 48비트의 데이터 중에 하나를 선택하는 멀티플렉서(710)와, 상기 멀티플렉서(710)에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 S-Box(720)와, 제어기의 제어를 받아 상기 4비트의 데이터를 네개로 분배하는 디멀티플렉서(730)와, 제1클럭(CLK_A)과 제2클럭(CLK_B)를 입력받아 상기 멀티플렉서와 디멀티플렉서를 제어하는 제어기(740)를 구비한다.

<39> 이상에서 살펴본 종래기술은 도6에서 도시된 것과 같이 네 개의 입력에 대하여 물리적으로 각각 다른 경로로 데이터를 전달하여 주어진 시간에서 동시에 4 개씩 억세스(Access)할 때 발생되는 데이터 컨텐션(Contention) 문제를 해결할 수 있으나, 똑 같은 S-Box 치환부 네 개를 사용함으로써 면적이 증가되는 문제점이 발생한다

<40> 또한 도7에서 제시한 종래 기술은 도6에서 제시한 S-Box 보다 면적을 1/4로 축소시켰으나 성능이 1/4로 감소하는 문제점이 발생한다.

【발명이 이루고자 하는 기술적 과제】

<41> 본 발명은 상기와 같은 종래기술의 문제점을 해결하기 위하여 안출된 것으로써, 면적을 최소화하고 성능을 증대시킬 수 있는 암호화 장치를 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<42> 상기 목적을 달성하기 위하여 본 발명의 암호화 장치는 데이터 암호화 표준 알고리즘을 사용하여 암호화를 수행하는 암호화 장치에 있어서, 제1제어기의 제어를 받아 입력되는 48 비트의 제1입력과 제2입력 중에서 하나를 선택하는 제1멀티플렉서; 상기 제1멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 제1S-Box; 제1제어기의 제어를 받아 상기 4비트의 데이터를 두개로 분배하는 제1디멀티플렉서; 제1클럭과 제2클럭을 입력받아 상기 제1멀티플렉서와 제1디멀티플렉서를 제어하는 제1제어기; 제2제어기의 제어를 받아 입력되는 48 비트의 제3입력과 제4입력 중에서 하나를 선택하는 제2멀티플렉서; 상기 제2멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 제2S-Box; 제2제어기의 제어를 받아 상기 4비트의 데이터를 두개로 분배하는 제2디멀티플렉서; 제1클럭과 제2클럭를 입력받아 상기 제2멀티플렉서와 제2디멀티플렉서를 제어하는 제2제어기를 포함하여 이루어진다.

<43> 본 발명은 S-Box 치환부에서 4 배 빠른 기억 장치를 구현하기 어려운 경우 2 배 빠른 기억 장치 두개를 사용하여 2-포트 S-Box 치환부를 구현함으로써 면적은 상기 도6에

서 제시한 S-Box 치환부보다 1/2로 축소되고, 성능은 상기 도7에서 도시된 S-Box 치환부보다 두 배가 증가한다.

<44> 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 가장 바람직한 실시예를 첨부한 도면을 참조하여 설명하기로 한다.

<45> 도8은 본 발명의 두 개의 2-포트 S-Box 치환부를 나타내는 블럭도이다.

<46> 상기 도8을 참조하면, 본 발명의 두개의 2-포트 S-Box 치환부는 제1제어기의 제어를 받아 입력되는 48 비트의 제1입력과 제2입력 중에서 하나를 선택하는 제1멀티플렉서(810)와, 상기 제1멀티플렉서(810)에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 제1S-Box(820)와, 제1제어기의 제어를 받아 상기 4비트의 데이터를 두개로 분배하는 제1디멀티플렉서(830)와, 제1클럭(CLK_A)과 제2클럭(CLK_B)를 입력받아 상기 제1멀티플렉서와 제1디멀티플렉서를 제어하는 제1제어기(840)와, 제2제어기의 제어를 받아 입력되는 48 비트의 제3입력과 제4입력 중에서 하나를 선택하는 제2멀티플렉서(850)와, 상기 제2멀티플렉서(850)에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 제2S-Box(860)와, 제2제어기의 제어를 받아 상기 4비트의 데이터를 두개로 분배하는 제2디멀티플렉서(870)와, 제1클럭(CLK_A)과 제2클럭(CLK_B)를 입력받아 상기 제2멀티플렉서와 제2디멀티플렉서를 제어하는 제2제어기(880)을 구비한다.

<47> 도9은 종래 방식의 단일 포트 S-Box 치환부와 4 포트 S-Box 치환부 그리고

본 발명의 2-포트 S-Box의 동작을 나타내는 타이밍도이다.

<48> 상기 도9을 참조하면, 본 발명에서는 제어기에 입력되는 두 배가 빠른 제1클럭(CLK_A)과 제2클럭(CLK_B)을 이용하여 롬(ROM)을 엑세스(Access)하는데 필요한 신호들을 발생시킨다. 각 시간 구간 t_i-t_{i+1}에서 제1경로(path1)와 제2경로(path2), 또는 제3경로(path3)와 제4경로(path4) 중의 한 경로를 선택하는 멀티플렉서에 의해 시분할된 제1경로(path1)와 제2경로(path2) 또는 제3경로(path3)와 제4경로(path4)가 개념적으로 존재하여 데이터 컨텐션(Data Contention) 문제를 해결한다. 즉, 제1클럭(CLK_A)가 논리 하이일 때 제1경로(path1)을 선택하여 b_i값들이 계산되고 제2클럭(CLK_B)가 하이일 때 제2경로(path2)를 선택하여 d_i값들이 계산된다. 또한, 제1클럭(CLK_A)가 논리 하이일 때 제3경로(path1)을 선택하여 f_i값들이 계산되고 제2클럭(CLK_B)가 하이일 때 제4경로(path2)를 선택하여 h_i값들이 계산된다.

<49> 본 발명의 기술 사상은 상기 바람직한 실시예에 따라 구체적으로 기술되었으나 상기한 실시예는 그 설명을 위한 것이며 그 제한을 위한 것이 아님을 주의하여야 한다. 또한, 본 발명의 기술 분야의 통상의 전문가라면 본 발명의 기술 사상의 범위내에서 다양한 실시예가 가능함을 이해할 수 있을 것이다.

【발명의 효과】

<50> 상기와 같이 본 발명은 2-포트 S-Box 치환부를 두 개 사용함으로써, S-Box 치환부가 차지하는 면적을 종래기술에 비해서 1/2로 축소하였고, 성능을 두 배로 증가시켰다.

또한 여러 형태의 DES 아키텍처를 구현하여 성능과 면적을 최적화할 수 있는 선택의 범위를 증대시킨다.

【특허청구범위】

【청구항 1】

데이터 암호화 표준 알고리즘을 사용하여 암호화를 수행하는 암호화 장치에 있어서,

제 1제어기의 제어를 받아 입력되는 48 비트의 제1입력과 제2입력 중에서 하나를 선택하는 제1멀티플렉서;

상기 제1멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 제1S-Box;

제어기의 제어를 받아 상기 4비트의 데이터를 두개로 분배하는 제1디멀티플렉서;

제1클럭과 제2클럭을 입력받아 상기 제1멀티플렉서와 제1디멀티플렉서를 제어하는 제1제어기;

제 2제어기의 제어를 받아 입력되는 48 비트의 제3입력과 제4입력 중에서 하나를 선택하는 제2멀티플렉서;

상기 제2멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 제2S-Box;

제어기의 제어를 받아 상기 4비트의 데이터를 두개로 분배하는 제2디멀티플렉서; 및

제1클럭과 제2클럭를 입력받아 상기 제1멀티플렉서와 제1디멀티플렉서를 제어하는 제2제어기

를 포함하여 이루어진 암호화 장치.

【청구항 2】

제 1 항에 있어서,

상기 제1클럭과 제2클럭은 서로 반전된 신호임을 특징으로 하는 암호화 장치.

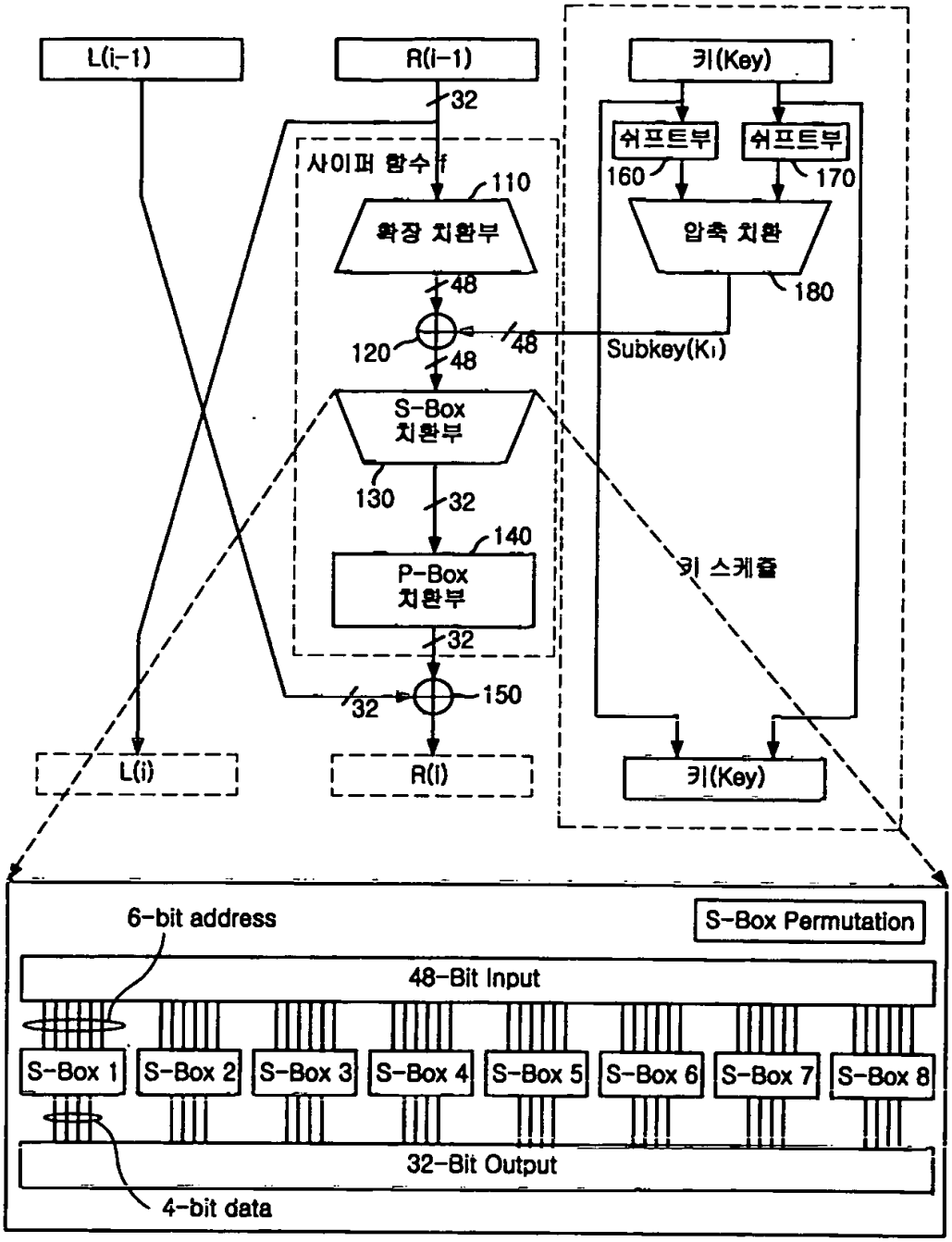
【청구항 3】

제 1 항에 있어서,

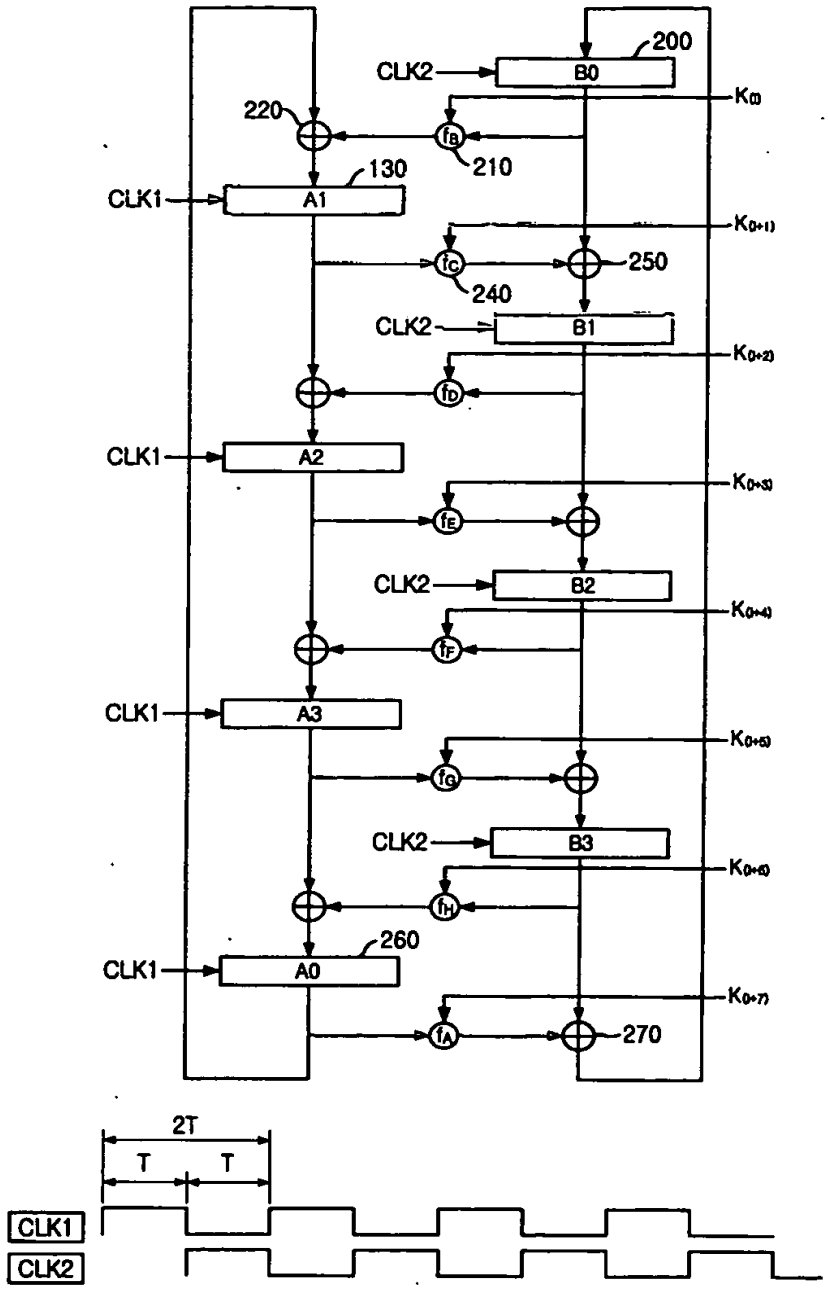
상기 제1멀티플렉서와 제1디멀티플렉서와 제2멀티플렉서와 제2디멀티플렉서는 물리적으로 존재하는 두개의 입력과 출력 경로를 시분할하여 데이터의 충돌을 방지하는 것임을 특징으로 하는 암호화 장치.

【도면】

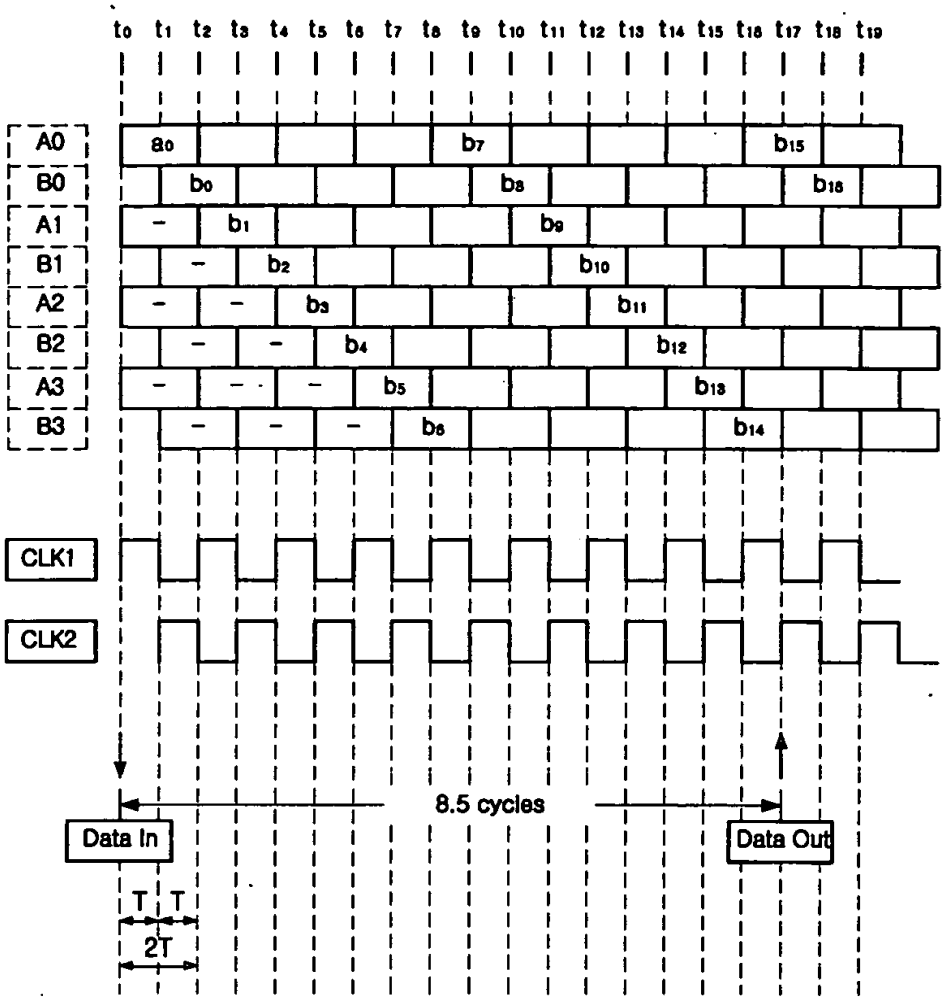
【도 1】


L(i-1)
R(i-1)
키(Key)
32
사이퍼 함수 f
쉬프트부
쉬프트부
160
170
110
확장 치환부
압축 치환
48
180
120
48
48
Subkey(Ki)
S-Box
치환부
130
32
140
P-Box
치환부
키 스케줄
32
32
150
L(i)
R(i)
키(Key)
6-bit address
S-Box Permutation
48-Bit Input
S-Box 1
S-Box 2
S-Box 3
S-Box 4
S-Box 5
S-Box 6
S-Box 7
S-Box 8
32-Bit Output
4-bit data

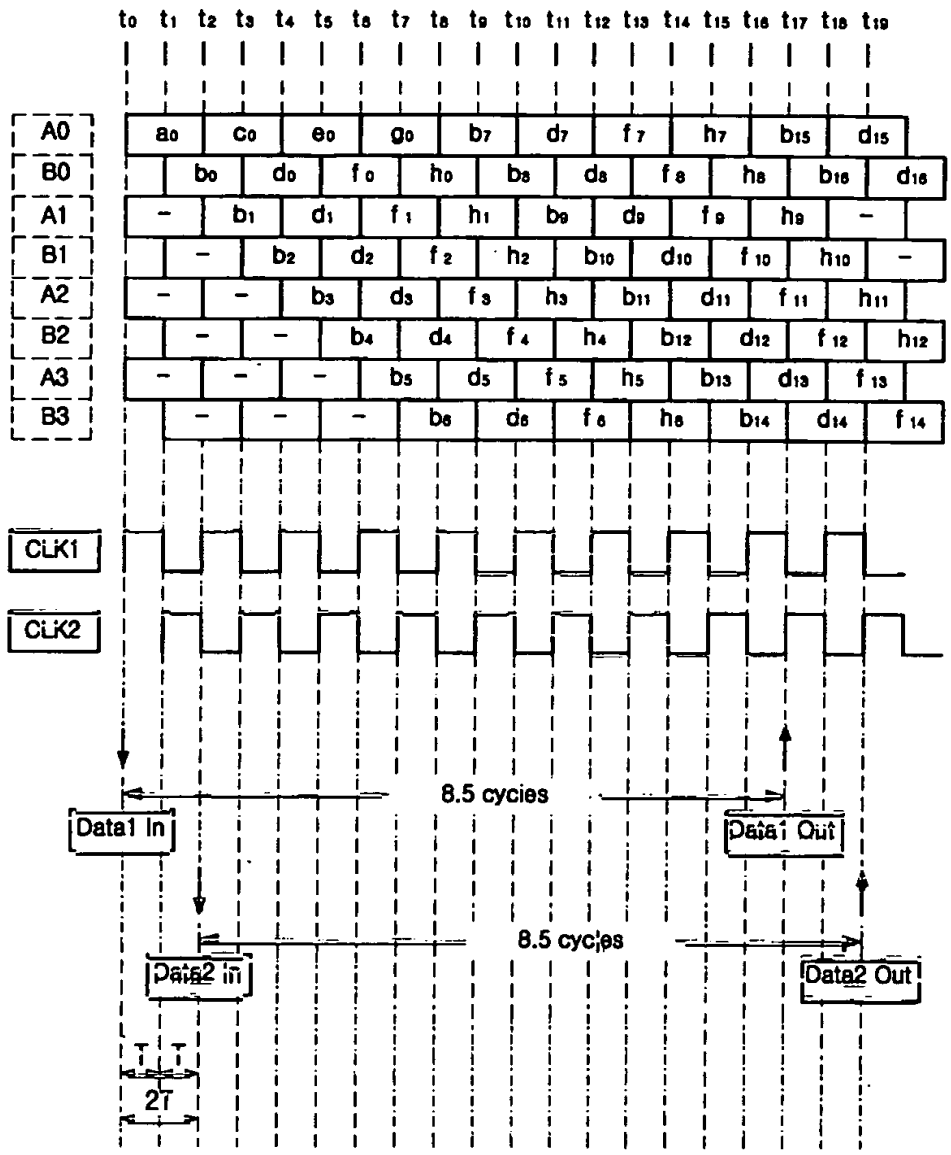
【도 2】


CLK2
B0
200
220
130
CLK1
A1
210
250
240
B1
A2
B2
A3
B3
260
A0
270
2T
T
T
CLK1
CLK2

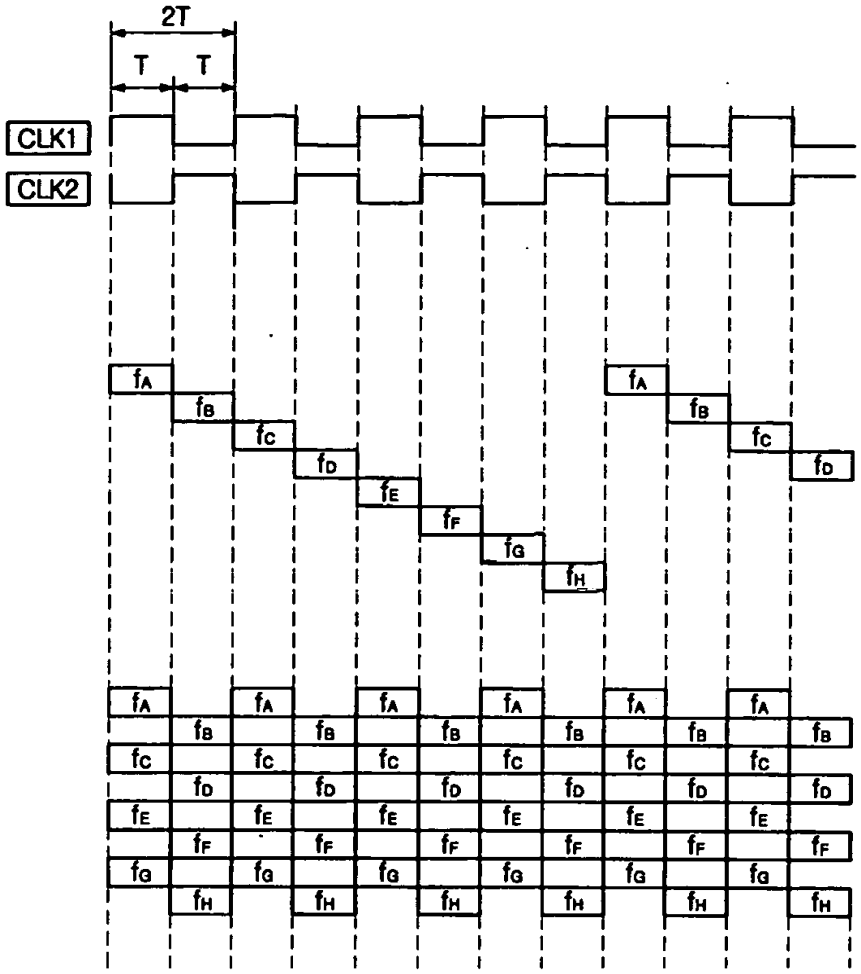
【도 3】


t0 t1 t2 t3 t4 t5 t6 t7 t8 t9 t10 t11 t12 t13 t14 t15 t16 t17 t18 t19
A0
B0
A1
B1
A2
B2
A3
B3
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 b10 b11 b12 b13 b14 b15
CLK1
CLK2
8.5 cycles
Data In
Data Out
T T
2T

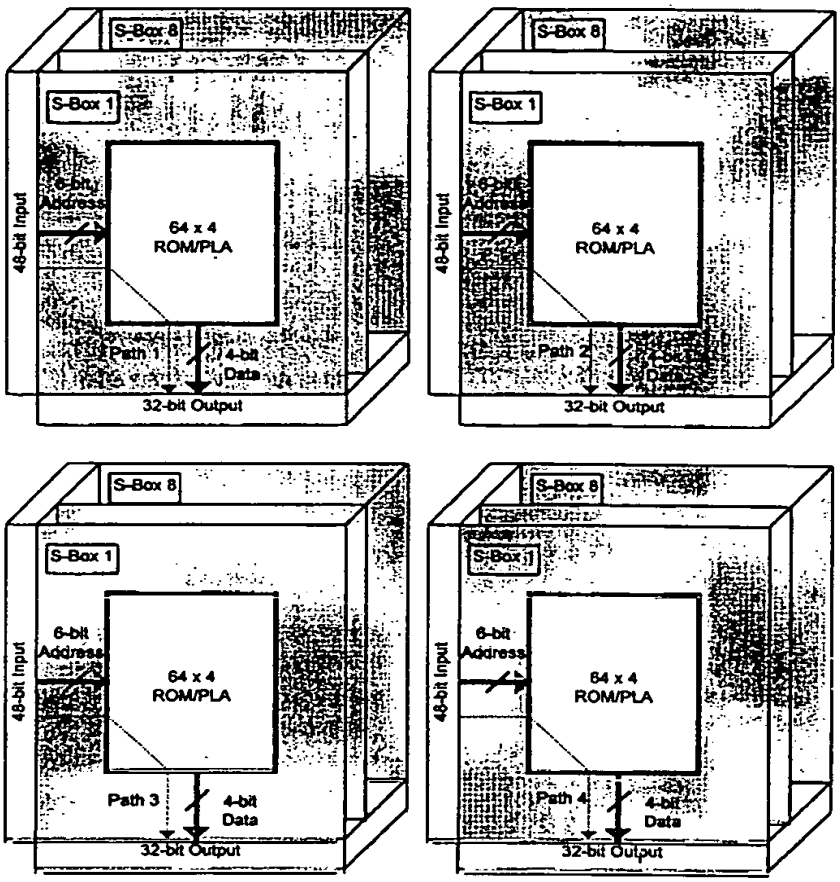
【도 4】


t0 t1 t2 t3 t4 t5 t6 t7 t8 t9 t10 t11 t12 t13 t14 t15 t16 t17 t18 t19
A0
B0
A1
B1
A2
B2
A3
B3
CLK1
CLK2
8.5 cycles
Data1 In
Data1 Out
8.5 cycles
Data2 In
Data2 Out
T
T
2T

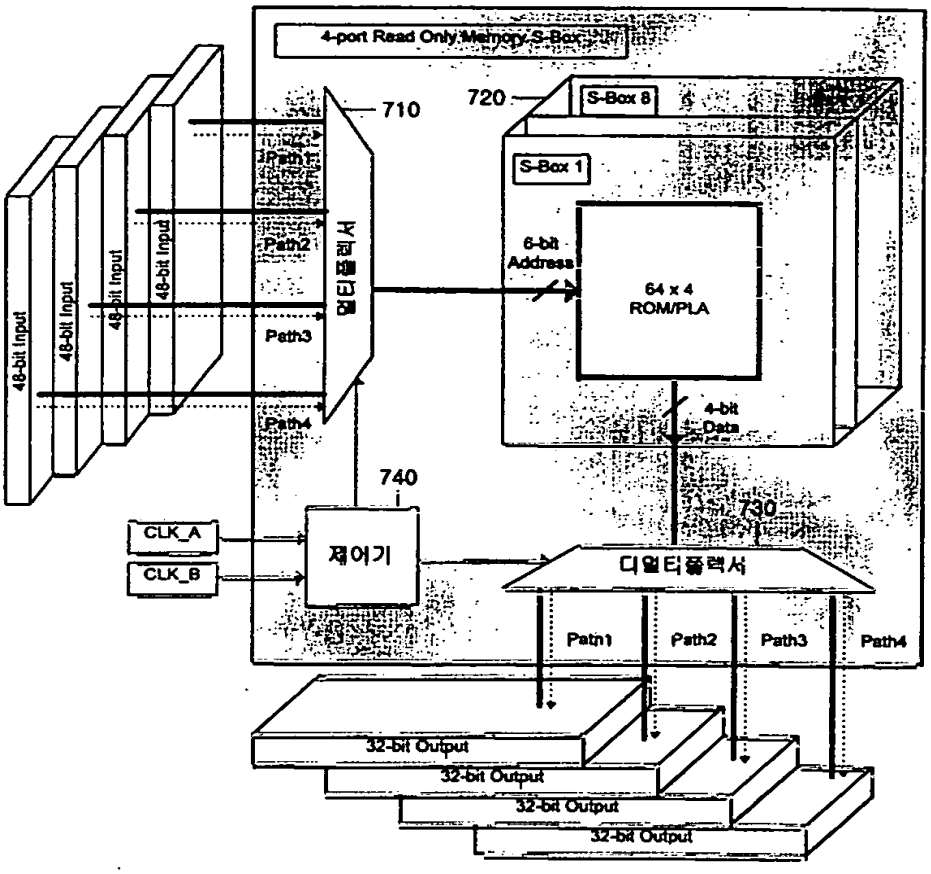
【도 5】



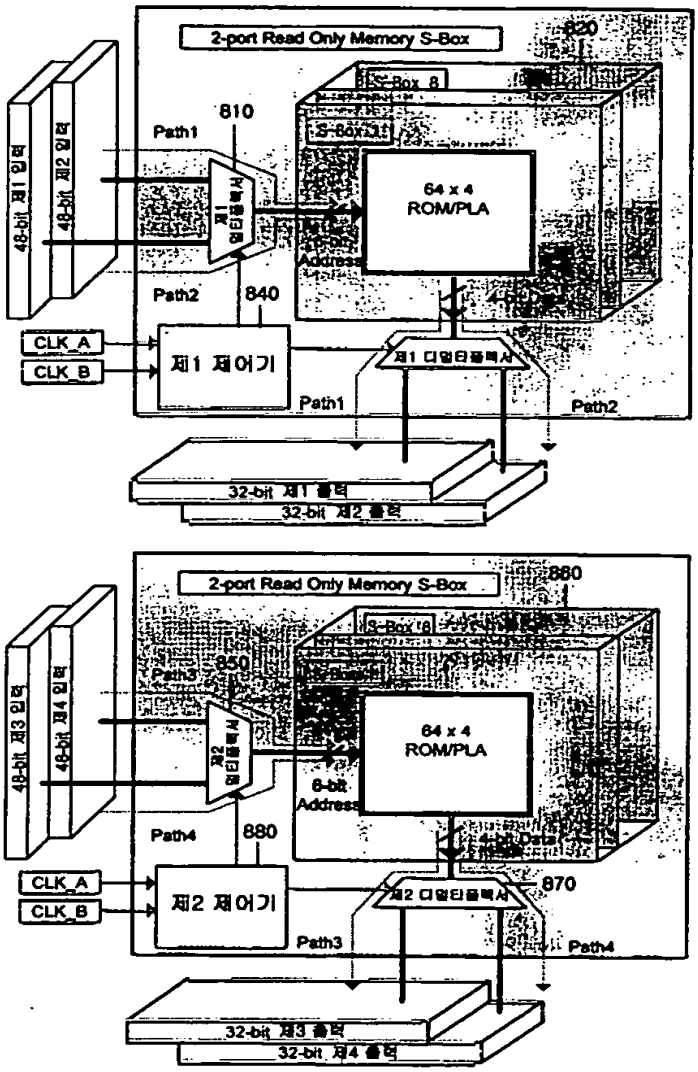
【도 6】


S-Box 8
S-Box 1
6-bit Address
64 x 4 ROM/PLA
48-bit Input
Path 1
4-bit Data
32-bit Output
S-Box 8
S-Box 1
64 x 4 ROM/PLA
48-bit Input
Path 2
32-bit Output
S-Box 8
S-Box 1
6-bit Address
64 x 4 ROM/PLA
48-bit Input
Path 3
4-bit Data
32-bit Output
S-Box 8
S-Box 1
6-bit Address
64 x 4 ROM/PLA
48-bit Input
Path 4
4-bit Data
32-bit Output

【도 7】


4-port Read Only Memory S-Box
710
720
S-Box 8
S-Box 1
48-bit Input
48-bit Input
48-bit Input
48-bit Input
Path1
Path2
Path3
Path4
멀티플렉서
6-bit Address
64 x 4 ROM/PLA
4-bit Data
740
730
CLK_A
CLK_B
제어기
디멀티플렉서
Path1
Path2
Path3
Path4
32-bit Output
32-bit Output
32-bit Output
32-bit Output

【도 8】


2-port Read Only Memory S-Box
820
S-Box 8
S-Box 31
810
Path1
48-bit 제1 입력
48-bit 제2 입력
64 x 4
ROM/PLA
6-bit
Address
Path2
840
CLK_A
CLK_B
제1 제어기
제1 다일터플렉서
Path1
Path2
32-bit 제1 출력
32-bit 제2 출력
2-port Read Only Memory S-Box
860
S-Box 8
S-Box 31
850
Path3
48-bit 제3 입력
48-bit 제4 입력
64 x 4
ROM/PLA
6-bit
Address
Path4
880
CLK_A
CLK_B
제2 제어기
870
제2 다일터플렉서
Path3
Path4
32-bit 제3 출력
32-bit 제4 출력

【도 9】